Security Tips

Be careful what you share

Never put anything truly sensitive on a social media site: Social Security numbers, date of birth, your exact home address, phone numbers, credit card or banking information of any kind, or detailed information on close family members. This will help to avoid a thief compromising your identity.

Weekly virus scans help keep you safe

It can take hours to months before the antivirus companies know about a new virus or piece of malware. In that time, that malware might make it onto your computer. By running weekly scans, when the antivirus companies are able to send out updates to address a piece of malware, your machine will have a chance to catch any malware that slipped in before the update was available. Real-time protection is important, but weekly scans are just as important.

Ready to get rid of that old hard drive or flash drive?

Not so fast! Make certain all of the data has been removed from the drive before throwing it in the trash or giving it away. Secure deletion of data requires more than just clicking "delete".

Be careful where you enter that information...

Many websites place their forms on pages that are not secured against evesdropping. Check to make certain you are entering your login information or purchase information on a page that has SSL security enabled. Otherwise, someone else may be able to read that information as it sent across the internet.

Unplug that flash drive!

USB flash drives (thumb drives), external hard drives and even DVD's can be used to spread a computer virus or malware. If you are going to connect a drive to your computer or pop in a DVD, wait until your computer is started, you are logged in and you are certain your anti-virus software is running before plugging in the drive. Be certain to unplug the drive or eject the disc when you are done.

This may help you avoid catching that bug hiding out in the drive.

Cached passwords and logins

Did you know that some sites keep you logged in via cookies even after you logout? After you are done with a browser in a public space, you should **close the browser**. This should make all session-specific cookies expire- keeping you a little safer online.

Lock your screen when you leave your desk

You should log out of your laptop or workstation if you leave your work area. But if you working on something important and don't want to lose your work, just lock the screen. In **Windows**, use the **CTRL+ALT+DEL** and choose the lock screen button**.** On the **Mac**, enable **Hot Corners** in your screen saver settings and set your computer to **require a password for sleep and screensaver** in **Security and Privacy**.

Remember: Not everything you read online is true

Don't believe everything you read on Facebook or other social sites: Scammers who have broken the security of one of your friends accounts will quickly contact all other "friends" with phishing or other scam emails that seem to come from someone you know and trust.

Be careful what you share

Never put anything truly sensitive on a social media site: Social Security numbers, your exact home address, phone numbers, credit card or banking information of any kind, or detailed information on close family members could all help a thief compromise your identity.

Back Up Your Data

Backup your data regularly to an external hard drive. You'll be protected from hard drive failures and laptop theft.

Guard your personal information

Don't give out your personal information to anyone unless you're sure they are who they say they are and that they need access to that information. This includes logins, passwords, email addresses, credit card information, and more.